**CMA ASS1**

**Q1.**

Cloud computing is on-demand access, via the internet, to computing resources—applications, servers (physical servers and virtual servers), data storage, development tools, networking capabilities, and more—hosted at a remote [data centre](https://www.ibm.com/in-en/cloud/learn/data-centers) managed by a cloud services provider (or CSP). The CSP makes these resources available for a monthly subscription fee or bills them according to usage. The formal definition of cloud computing comes from the National Institute of Standards and Technology (NIST): ​

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.​

Compared to traditional on-premises IT, and depending on the cloud services you select, cloud computing helps do the following:

* Lower IT costs: Cloud lets you offload some or most of the costs and effort of purchasing, installing, configuring, and managing your own on-premises infrastructure.
* Improve agility and time-to-value: With cloud, your organization can start using enterprise applications in minutes, instead of waiting weeks or months for IT to respond to a request, purchase and configure supporting hardware, and install software.
* Scale more easily and cost-effectively: Cloud provides elasticity—instead of purchasing excess capacity that sits unused during slow periods, you can scale capacity up and down in response to spikes and dips in traffic.

Deployment model

There are four main types: public, private, hybrid and community clouds. Additionally, there are also distributed clouds that are not as widespread, such as multiclouds, poly clouds and other models.

A **cloud deployment model** is a specific configuration of environment parameters such as the accessibility and proprietorship of the deployment infrastructure and storage size. This means that deployment types vary depending on who controls the infrastructure and where it’s located. To make the most use of this computing type, a company should opt for a model that suits it best.

#### Public Cloud

The public cloud allows systems and services to be easily accessible to the general public. Public cloud may be less secure because of its openness.

#### Private Cloud

The private cloud allows systems and services to be accessible within an organization. It is more secured because of its private nature.

#### Community Cloud

The community cloud allows systems and services to be accessible by a group of organizations.

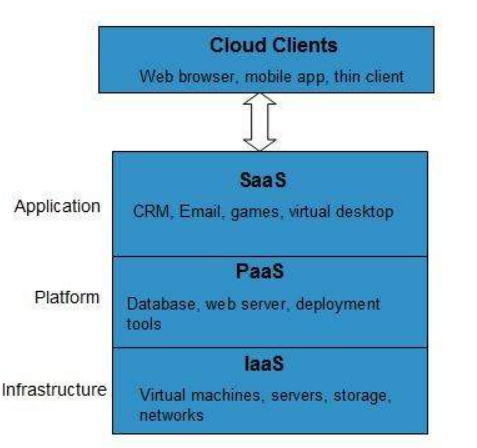
#### Hybrid Cloud

The hybrid cloud is a mixture of public and private cloud, in which the critical activities are performed using private cloud while the non-critical activities are performed using public cloud.

### Service Models

Cloud computing is based on service models. These are categorized into three basic service models which are -

* Infrastructure-as–a-Service (IaaS)
* Platform-as-a-Service (PaaS)
* Software-as-a-Service (SaaS)

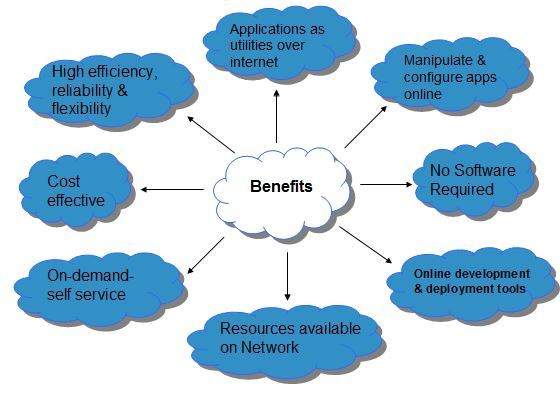


1. **Software-as-a-service (SaaS)** involves the licensure of a software application to customers. Licenses are typically provided through a pay-as-you-go model or on-demand. This type of system can be found in Microsoft Office's 365.1﻿
2. **Infrastructure-as-a-service (IaaS)** involves a method for delivering everything from operating systems to servers and storage through IP-based connectivity as part of an on-demand service. Clients can avoid the need to purchase software or servers, and instead procure these resources in an [outsourced](https://www.investopedia.com/terms/o/outsourcing.asp), on-demand service. Popular examples of the IaaS system include IBM Cloud and Microsoft Azure.2﻿ 3﻿
3. **Platform-as-a-service (PaaS)** is considered the most complex of the three layers of cloud-based computing. PaaS shares some similarities with SaaS, the primary difference being that instead of delivering software online, it is actually a platform for creating software that is delivered via the Internet. This model includes platforms like Salesforce.com and Heroku

## Benefits

Cloud Computing has numerous advantages. Some of them are listed below -

* One can access applications as utilities, over the Internet.
* One can manipulate and configure the applications online at any time.
* It does not require to install a software to access or manipulate cloud application.
* Cloud Computing offers online development and deployment tools, programming runtime environment through PaaS model.
* Cloud resources are available over the network in a manner that provide platform independent access to any type of clients.
* Cloud Computing offers on-demand self-service. The resources can be used without interaction with cloud service provider.
* Cloud Computing is highly cost effective because it operates at high efficiency with optimum utilization. It just requires an Internet connection
* Cloud Computing offers load balancing that makes it more reliable.



## Risks related to Cloud Computing

Although cloud Computing is a promising innovation with various benefits in the world of computing, it comes with risks. Some of them are discussed below:

### Security and Privacy

It is the biggest concern about cloud computing. Since data management and infrastructure management in cloud is provided by third-party, it is always a risk to handover the sensitive information to cloud service providers.

Although the cloud computing vendors ensure highly secured password protected accounts, any sign of security breach may result in loss of customers and businesses.

### Lock In

It is very difficult for the customers to switch from one Cloud Service Provider (CSP) to another. It results in dependency on a particular CSP for service.

### Isolation Failure

This risk involves the failure of isolation mechanism that separates storage, memory, and routing between the different tenants.

### Management Interface Compromise

In case of public cloud provider, the customer management interfaces are accessible through the Internet.

### Insecure or Incomplete Data Deletion

It is possible that the data requested for deletion may not get deleted. It happens because either of the following reasons

* Extra copies of data are stored but are not available at the time of deletion
* Disk that stores data of multiple tenants is destroyed.

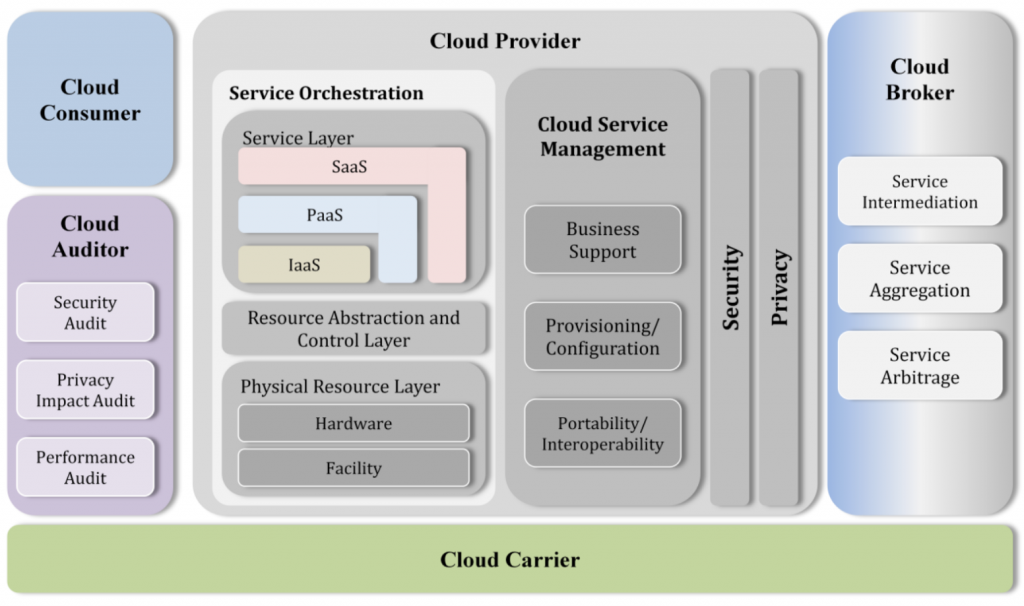
The [National Institute of Standards and Technology](https://en.wikipedia.org/wiki/National_Institute_of_Standards_and_Technology)'s definition of cloud computing identifies "five essential characteristics":

1. **On-demand self-service:** A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
2. **Broad network access:** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., [**mobile**](https://www.govinfosecurity.com/mobility-c-212) phones, tablets, laptops and workstations).
3. **Resource pooling:** The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state or datacenter). Examples of resources include storage, processing, memory and network bandwidth.
4. **Rapid elasticity:** Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
5. **Measured service:** Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth and active user accounts). Resource usage can be monitored, controlled and reported, providing transparency for the provider and consumer.

**Q2. Cloud Computing conceptual reference model**

**Cloud computing conceptual reference model identifies the major actors, their activities and functions in cloud computing.**

**Below figure 1 presents an overview of the NIST cloud reference architecture.**

****

**Figure 1 – The Conceptual Reference Model**

**As shown in Figure 1, the NIST cloud computing reference architecture defines five major actors: cloud consumer, cloud provider, cloud carrier, cloud auditor and cloud broker. Each actor is an entity (a person or an organization) that participates in a transaction or process and/or performs tasks in cloud computing.**

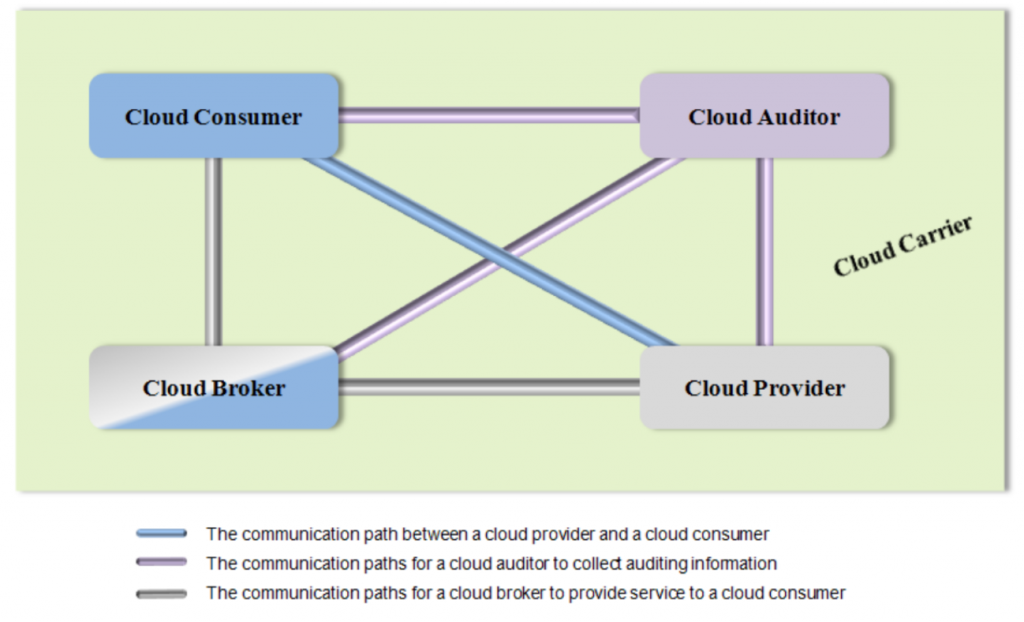
**Table 1 briefly lists the actors defined in the NIST cloud computing reference architecture. The general activities of the actors are discussed in further tutorial.**

**Actors in Cloud Computing**

|  |  |  |
| --- | --- | --- |
| SNO | Actor | Definition |
| 1 | **Cloud Consumer** | **A person or organization that maintains a business relationship with, and uses service from, Cloud Providers.** |
| 2 | **Cloud Provider** | **A person, organization, or entity responsible for making a service available to interested parties.** |
| 3 | **Cloud Auditor** | **A party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation.** |
| 4 | **Cloud Broker** | **An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between Cloud Providers and Cloud Consumers.** |
| 5 | **Cloud Carrier** | **An intermediary that provides connectivity and transport of cloud services from Cloud Providers to Cloud Consumers.** |

**Table 1 – Actors in Cloud Computing**

**Figure 2 illustrates the interactions among the actors. A cloud consumer may request cloud services from a cloud provider directly or via a cloud broker. A cloud auditor conducts independent audits and may contact the others to collect necessary information. The details will be discussed in the following sections and presented in increasing level of details in successive diagrams.**

****

**Figure 2 Interactions between the Actors in Cloud Computing**

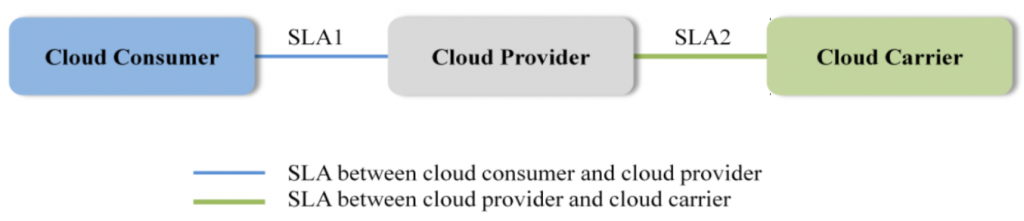
**Usage Scenario 1: A cloud consumer may request service from a cloud broker instead of contacting a cloud provider directly. The cloud broker may create a new service by combining multiple services or by enhancing an existing service. In this example, the actual cloud providers are invisible to the cloud consumer and the cloud consumer interacts directly with the cloud broker.**

****

**Figure 3 Usage Scenario for Cloud Brokers**

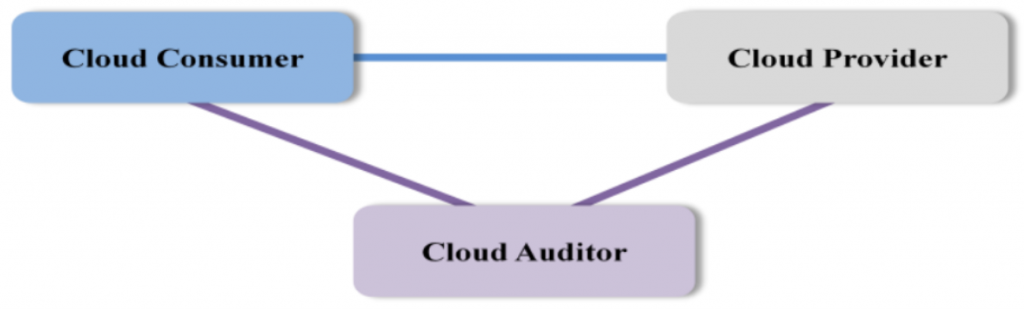
**Usage Scenario 2: Cloud carriers provide the connectivity and transport of cloud services from cloud providers to cloud consumers. As illustrated in Figure 4, a cloud provider participates in and arranges for two unique service level agreements (SLAs), one with a cloud carrier (e.g. SLA2) and one with a cloud consumer (e.g. SLA1).**

**A cloud provider arranges service level agreements (SLAs) with a cloud carrier and may request dedicated and encrypted connections to ensure the cloud services are consumed at a consistent level according to the contractual obligations with the cloud consumers. In this case, the provider may specify its requirements on capability, flexibility and functionality in SLA2 in order to provide essential requirements in SLA1.**

****

**Figure 4 Usage Scenario for Cloud Carriers**

**Usage Scenario 3: For a cloud service, a cloud auditor conducts independent assessments of the operation and security of the cloud service implementation. The audit may involve interactions with both the Cloud Consumer and the Cloud Provider.**

****

<https://timesofcloud.com/cloud-tutorial/cloud-consumer/>

Q.3 . Private Cloud

1. There is little to no difference between a public and a private model from the technical point of view, as their architectures are very similar. However, as opposed to a public cloud that is available to the general public, only one specific company owns a private cloud. That is why it is also called an *internal* or *corporate* model.

The server can be hosted externally or on the premises of the owner company. Regardless of their physical location, these infrastructures are maintained on a designated private network and use software and hardware that are intended for use only by the owner company.

A clearly defined scope of people have access to the information kept in a private repository, which prevents the general public from using it. In light of numerous breaches in recent years, a growing number of large corporations has decided on a closed private cloud model, as this minimizes data security issues.

Compared to the public model, the private cloud provides wider opportunities for customizing the infrastructure to the company’s requirements. A private model is especially suitable for companies that seek to safeguard their mission-critical operations or for businesses with constantly changing requirements.

Multiple public cloud service providers, including Amazon, IBM, Cisco, Dell and Red Hat, also provide private solutions.

At SaM Solutions, we have created an efficient ready-to-use Platform as a Service, the [SaM CloudBOX](https://www.sam-solutions.com/services/sam-cloudbox-paas/). This PaaS facilitates projects via quick and easy launching and allows companies to make the most of BizDevOps.

Essentials of cloud computing (2015).pdf **SLIDE NO 71**

1. **IAAS**

Essentials of cloud computing (2015).pdf **SLIDE 97**